James E. Cecchi
CARELLA BYRNE CECCHI
BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
jcecchi@carellabyrne.com

Attorney for Plaintiff and the putative Class

[Additional Attorneys on Signature Page]

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

ALLAN BISHOP, Individually And On Behalf Of All Others Similarly Situated, Plaintiff, v. HEALTHEC LLC, Defendant.	Case No.: _____ **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Allan Bishop ("Plaintiff"), by and through undersigned counsel, files this Class Action Complaint individually and on behalf of a class of all similarly situated persons against HealthEC LLC ("Defendant" or "HEC"). Plaintiff bases the following allegations upon information and belief, investigation of counsel, and his own personal knowledge.

NATURE OF THE ACTION

1. Healthcare providers and their business associates who handle sensitive, personally identifiable information ("PII") or protected health information ("PHI") owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII or PHI to unauthorized persons—especially to hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health

matters.

2. The harm resulting from a data and privacy breach manifests in a number of ways, such as identity theft and financial fraud, and the exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional precautionary measures.

3. HEC is a healthcare technology company based in New Jersey. HEC provides an AI-enabled population health manager (PHM) platform used by over one million healthcare professionals across its client organizations.

4. As a healthcare business associate of its client healthcare organizations, HEC knowingly obtains sensitive patient PII and PHI from its members and, thus, has the resulting duty to securely maintain such information in confidence.

5. HEC expressly recognizes this duty, pledging an "ongoing commitment to your privacy and the security of information in our care."[1]

6. Despite HEC's duty to safeguard the PII and PHI of its members, Plaintiff's and Class Members' sensitive information was exposed to unauthorized third parties during a massive data breach that occurred between July 14, 2023 and July 23, 2023 (the "Data Breach" or "Breach" herein).

7. The Data Breach impacted 4.5 million patients across 17 healthcare service

[1] *Data Breach Notice Letter*, HEC (Dec. 22, 2023), https://www.healthec.com/cyber-incident/ ("Notice").

providers and state-level health systems that use HEC's technology services.[2]

8. Although the Data Breach occurred in July, HEC waited approximately five months to notify individuals impacted by the Breach. Indeed, Defendant waited until on or about December 22, 2023 to begin notifying individuals that their PII and PHI had been compromised.[3]

9. Based on the information publicly available to date, a wide variety of PII and PHI was implicated in the Data Breach, including, *inter alia*, individuals' names, addresses, dates of birth, Social Security numbers, taxpayer identification numbers, medical record numbers, medical information (including medical diagnoses, providers' names and locations, and prescription information), health insurance information (including beneficiary numbers, subscriber numbers, and Medicare/Medicaid identification information), and billing and claims information (including patient account numbers).[4]

10. As a direct and proximate result of Defendant's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII and PHI is now in the hands of cybercriminals.

11. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, and intrusion of their health privacy—risk which may last for the rest of their lives. Consequently, Plaintiff and Cloass Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

---

[2] Bill Toulas, *Data Breach at Healthcare Tech Firm Impacts 4.5 Million Patients*, Bleeping Computer (Jan. 3, 2024), https://www.bleepingcomputer.com/news/security/data-breach-at-healthcare-tech-firm-impacts-45-million-patients/.
[3] Notice, *supra* note 1; Steve Alder, *HealthEC Data Breach Affects Almost 4.5 Million Individuals*, HIPAA J. (Jan. 3, 2024), https://www.hipaajournal.com/healthec-data-breach/.
[4] Notice, *supra* note 1.

12. Plaintiff, on behalf of himself and all others similarly situated, alleges claims for negligence, negligence *per se*, and declaratory judgment. Plaintiff seeks damages and injunctive relief, including the adoption of reasonably sufficient practices to safeguard PII and PHI in Defendant's custody in order to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

13. Plaintiff Allan Bishop is an adult who, at all relevant times, is a resident of the State of Florida. Plaintiff received Notice of the Data Breach from Defendant, in which Plaintiff was informed that his PII and PHI in Defendant's possession had been exposed during the Breach.

14. Defendant HealthEC LLC is a Delaware limited liability company that maintains its headquarters at 343 Thornall Street, Suite 630, Edison, New Jersey, 08837.

15. Upon information and belief, Defendant has five members—Ashish Kapoor, Steve Tolle, Enrico Picozza, Shilpa Nayyar, and Chris Caramanico—each of whom are citizens of the State of New Jersey.[5]

16. Defendant is a citizen of each state in which its members maintain citizenship. As such, Defendant is a citizen of New Jersey.

17. Plaintiff will amend his Complaint should additional or alternative limited liability company members be revealed.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because Plaintiff and at least

---

[5] Notice of Exempt Offering of Securities, HealthEC (October 10, 2023), https://www.sec.gov/Archives/edgar/data/1764061/000156761923007409/xslFormDX01/primary_doc.xml

one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

19. This Court has general personal jurisdiction over Defendant because, at all relevant times, HEC maintains its headquarters in New Jersey, is registered to conduct business in New Jersey, and has engaged in substantial business activities in New Jersey.

20. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) and (2) because a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred in this District, Defendant conducts substantial business within this District, and Defendant has harmed Class Members residing in this District. Further, upon information and belief, Defendant's members are all citizens of New Jersey.

FACTUAL BACKGROUND

A. Defendant and the Services it Provides.

21. HEC is a provider of health management technology services. Specifically, HEC offers an AI-enabled population health management (PHM) platform to healthcare organizations that "ingests all available data," including "clinical and claims data" to "create a community health record for each patient."[6] Healthcare organizations can then use HEC's platform for data integration, analytics, care coordination, patient engagement, compliance, and reporting.[7]

22. Upon information and belief, while administering its services, HEC receives, maintains, and handles patient PII and PHI. This information includes, *inter alia*, individuals' individuals' names, addresses, dates of birth, Social Security numbers, taxpayer identification

[6] HealthEC, https://www.healthec.com/.
[7] Toulas, *supra* note 2.

numbers, medical record numbers, medical information, health insurance information, and billing and claims information.

23. Plaintiff and Class Members directly or indirectly trusted HEC with their sensitive and confidential PII and PHI and therefore reasonably expected that Defendant would safeguard their highly sensitive PII and keep their PHI confidential.

24. Due to the sensitivity of the PII and PHI that HEC handles, it is aware of its critical responsibility to safeguard this information—and, therefore, how devastating its theft is to individuals whose information has been stolen.

25. By obtaining, collecting, and storing Plaintiff's and Class Members' PII and PHI, HEC assumed equitable and legal duties to safeguard and keep confidential Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

26. Despite the existence of these duties, HEC failed to implement reasonable data security measures to protect Plaintiff's and Class Members' PII and PHI, and ultimately allowed nefarious third-party hackers to compromise Plaintiff's and Class Members' PII and PHI.

B. Defendant is Subject to HIPAA as a Business Associate.

27. Upon information and belief, because HEC receives, maintains, and handles PII and PHI from healthcare providers, Defendant qualifies as a Business Associate within the meaning of 45 C.F.R. § 160.103(3), and has entered into Business Associate Contracts or Agreements with its clients to set forth its obligations as a custodian of patient PHI.

28. As a business associate, HEC is a covered entity under the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 1302d, et seq.

29. Under HIPAA, HEC is required to ensure the implementation of adequate

safeguards to prevent unauthorized use or disclosure of patients' information, including by implementing requirements of the HIPAA Security Rule, and are required to report any unauthorized use or disclosure of PII and/or PHI, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

30. Due to the nature of HEC's business, it would be unable to engage in regular business activities without collecting and aggregating patient information that it knows and understands to be sensitive and confidential.

31. HEC did not maintain adequate security to protect its systems from infiltration by cybercriminals, and subsequently waited months to publicly disclose the Data Breach.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' sensitive information, HEC assumed legal and equitable duties, and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII and/or PHI from unauthorized disclosure.

33. Further, given the application of HIPAA, and that Plaintiff and Class Members directly or indirectly entrusted their PHI to HEC in order to receive healthcare services, Plaintiff and Class Members reasonably expected that HEC would safeguard their highly sensitive information and keep their PHI confidential.

C. Defendant Knew the Risks of Storing Valuable PII and PHI.

34. HEC was well aware that the PII and PHI it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

35. HEC also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

36. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Facebook, Yahoo, Marriott, as well as healthcare companies such as Anthem and Delta Dental.

37. PII and PHI have considerable value and constitute enticing and well-known targets to hackers. Hackers can easily sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[8] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false claims for reimbursement.

38. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[9]

39. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[10]

40. The healthcare industry has become a prime target for threat actors: "[h]igh demand for patient information and often-outdated systems are among the nine reasons healthcare is now

---

[8] Brian Krebs, *The Value of a Hacked Company*, Krebs On Sec. (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.
[9] *Data Breach Report: 2021 Year End*, Risk Based Sec. (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/.
[10] *Facts + Statistics: Identity theft and cybercrime*, Ins. Info. Inst., https://www.iii.org/factstatistic/facts-statistics-identity-theft-andcybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Oct. 20, 2023).

the biggest target for online attacks."[11]

41. Additionally, "[h]ospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it quickly—making the industry a growing target."[12]

42. Cybercriminals seek out PHI at a greater rate than other sources of personal information. Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more individuals have been reported to Health and Human Services' Office of Civil Rights, resulting in the exposure or unauthorized disclosure if the information of 382,262,109 individuals—"[t]hat equates to more than 1.2x the population of the United States."[13]

43. Further, the rate of healthcare data breaches has been on the rise in recent years. "In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare data breaches of 500 or more records were reported each day."[14]

44. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[15]

45. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July 2022. The percentage of

---

[11] *The healthcare industry is at risk*, SwivelSecure, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Oct. 20, 2023).
[12] *Id.*
[13] *Healthcare Data Breach Statistics*, HIPAA J., https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Oct. 18, 2023).
[14] *Id.*
[15] *2022 Breach Barometer*, Protenus, https://www.protenus.com/breach-barometer-report (last visited Oct. 20, 2023).

healthcare breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[16]

46. The breadth of data compromised in the Data Breach here makes the information particularly valuable to thieves and leaves the patients of HEC's healthcare provider partners especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

47. **Social Security Numbers**—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique Social Security Numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

48. The Social Security Administration even warns that the process of replacing a Social Security is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new

[16] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

> number, the absence of any credit history under the new number may make more difficult for you to get credit.[17]

49. Social Security Numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit – among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

50. **Healthcare Records**—As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals – they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. 'Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to – we've even seen $60 or $70.'"[18] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[19]

51. Indeed, medical records "are so valuable because they can be used to commit a multitude of crimes. Healthcare data can be used to impersonate patients to obtain expensive medical services, Medicare and Medicaid benefits, healthcare devices, and prescription medications. Healthcare records also contain the necessary information to allow fraudulent tax

---

[17] *Identify Theft and Your Social Security Numbers*, Social Sec. Admin. (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf, (last visited Oct. 20, 2023).

[18] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, *New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat, (last visited Oct. 20, 2023).

[19] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, PriceWaterhouseCoopers (Sept. 30, 2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited Oct. 20, 2023).

returns to be filed to obtain rebates."[20]

52. "In contrast to credit card numbers and other financial information, healthcare data has an incredibly long lifespan and can often be misused for long periods undetected. Credit card companies monitor for fraud and rapidly block cards and accounts if suspicious activity is detected, but misuse of healthcare data is harder to identify and can be misused in many ways before any malicious activity is detected. During that time, criminals can run up huge debts – far more than is usually possible with stolen credit card information."[21]

53. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[22]

54. **Driver's License Numbers—**are highly sought after by cyber criminals on the dark

---

[20] Steve Adler, *Editorial: Why Do Criminals Target Medical Records*, HIPAA Journal. (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/#:~:text=Healthcare%20records%20are%20so%20valuable,credit%20cards%20in%20victims'%20names.

[21] *Id*.

[22] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (Mar. 31, 2023), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

web because they are unique to a specific individual and extremely sensitive. This is because a driver's license number is connected to an individual's vehicle registration, insurance policies, records on file with the DMV, places of employment, doctor's offices, government agencies, and other entities.

55. For these reasons, driver's license numbers are highly sought out by cyber criminals because they are one of the most valuable pieces of information to facilitate identity theft and fraud. This information is valuable because cyber criminals can use this information to open credit card accounts, obtain insurance policies and submit fraudulent claims, open cell phone contracts, file fraudulent tax returns, file unemployment applications, as well as obtain bank loans under a person's name.

56. Further, unlike credit or debit card numbers in a payment card data breach, which can quickly be frozen and reissued in the aftermath of a breach, the type of PII at stake here—unique driver's license numbers—cannot be easily replaced.

57. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[23]

58. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a

[23] U.S. Gov't Accountability Off., GAO-07-737, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (2007), https://www.gao.gov/new.items/d07737.pdf (last visited Oct. 20, 2023).

substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII and PHI about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

59. Based on the value of patients' PII and PHI to cybercriminals, HEC knew or should have known, the importance of safeguarding the PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. HEC failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

D. The Data Breach: Defendant Breached its Duty to Protect Individuals' PII and PHI.

60. On December 22, 2023, HEC posted and filed a notice of data breach ("Notice") indicating that the breach had occurred approximately five months previously, between July 14, 2023 and July 23, 2023.[24]

61. In the Notice, HEC describes the circumstances surrounding the Breach as follows:

> HEC became aware of suspicious activity potentially involving its network and promptly began an investigation. The investigation determined that certain systems were accessed by an unknown actor between July 14, 2023 and July 23, 2023, and during this time certain files were copied. We then undertook a thorough review of the files in order to identify what specific information was present in the files and to whom it relates. This review was completed on or around October 24, 2023 and identified information relating to some of HEC's clients. HEC began notifying our clients on October 26, 2023, and we worked with them to notify potentially impacted individuals.[25]

62. Upon information and belief, Class Members received similar Data Breach notices

[24] Notice, *supra* note 1.
[25] *Id.*

on or around the same time, informing them that their PII and/or PHI was exposed during the Data Breach.

63. According to HEC, this information included, *inter alia*, individuals':

a. Names;

b. Addresses;

c. Dates of birth;

d. Social Security numbers;

e. Taxpayer identification numbers;

f. Medical record numbers;

g. Medical information (including but not limited to diagnosis, diagnosis code, mental/physical condition, prescription information, and provider's name and location);

h. Health insurance information (including but not limited to beneficiary number, subscriber number, Medicaid/Medicare identification); and

i. Billing and claims information (including but not limited to patient account number, patient identification number, and treatment cost information).[26]

64. In sum, nearly 4.5 million individuals were impacted by the Data Breach across 17 different healthcare service providers and systems.[27]

65. This massive Data Breach occurred as a direct result of HEC's failure to implement and follow basic security procedures in order to protect the PII and PHI with which it had been entrusted.

E. Defendant is Obligated Under HIPAA to Safeguard Patient PII.

66. As a business associate of its Customer-Healthcare Providers, HEC is required by HIPAA to safeguard patient PHI.

---

[26] Notice, *supra* note 1.
[27] Toulas, *supra* note 2.

67. HEC is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

68. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

69. Under 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media;" "[m]aintained in electronic media;" or "[t]ransmitted or maintained in any other form or medium."

70. Under 45 C.F.R. § 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) "identifies the individual;" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual."

71. HIPAA requires HEC to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 C.F.R. §§ 164.102, *et seq*.

72. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires HEC to provide notice of the Data Breach to each affected individual "without unreasonable delay

and in no case later than 60 days following discovery of the breach."[28]

73. HHS further recommends the following data security measures a business associate such as HEC should implement to protect against some of the more common, and often successful, cyber-attack techniques. According to those guidelines, business associates should:

a. Implement security awareness and training for all workforce members and that the training programs should be ongoing, and evolving to be flexible to educate the workforce on new and current cybersecurity treats and how to respond;

b. Implement technologies that examine and verify that received emails do not originate from known malicious site, scan web links or attachments included in emails for potential threats, and impeded or deny the introduction of malware that may attempt to access PHI;

c. Mitigate known data security vulnerabilities by patching or upgrading vulnerable technology infrastructure, by upgrading or replacing obsolete and/or unsupported applications and devices, or by implementing safeguards to mitigate known vulnerabilities until an upgrade or replacement can occur;

d. Implement security management processes to prevent, detect, contain, and correct security violations, including conducting risk assessments to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI; and

e. Implement strong cyber security practices by requiring strong passwords rules and multifactor identification.[29]

74. Upon information and belief, Defendant failed to implement one or more of the recommended data security measures and timely notify Plaintiff and Class Members of a data breach impacting their PHI.

75. While HIPAA permits healthcare providers and their business associates to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers and

---

[28] *Breach Notification Rule*, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

[29] *OCR Quarter 1 2022 Cybersecurity Newsletter*, U.S. Dep't Health Hum.Servs., (Mar. 17, 2022), https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html.

their business associates to disclose PHI to cybercriminals nor did Plaintiff or the Class Members consent to the disclosure of their PHI to cybercriminals.

76. As such, HEC is required under HIPAA to maintain the strictest confidentiality of Plaintiff's and Class Members' PHI that it acquires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

77. Given the application of HIPAA to HEC, and that Plaintiff and Class Members directly or indirectly entrusted their PHI to Defendant in order to receive healthcare services from Defendant's Customer-Healthcare Providers, Plaintiff and Class Members reasonably expected that HEC would safeguard their highly sensitive information and keep their PHI confidential.

F. FTC Guidelines Prohibit Defendant from Engaging in Unfair or Deceptive Acts or Practices.

78. HEC is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

79. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[30]

80. Among other guidance, the FTC recommends the following cybersecurity

[30] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

guidelines for businesses in order to protect sensitive information in their systems: [31]

a. Identify all connections to the computers where sensitive information is stored;

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user.

---

[31] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

> If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

81. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[32]

82. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

83. HEC was at all times fully aware of its obligations to protect the PII and PHI of consumers because of its position as a business associate, which gave it direct access to reams of patient PII and PHI from its Customer-Healthcare Providers. HEC was also aware of the significant repercussions that would result from its failure to do so.

84. Despite its obligations, HEC failed to properly implement basic data security practices, and Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to member PII and PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

G. Plaintiff and Class Members Suffered Damages.

85. For the reasons mentioned above, HEC's conduct, which allowed the Data Breach

[32] *Id.*

to occur, caused Plaintiff and members of the Class significant injuries and harm in several ways. Plaintiff and members of the Class must immediately devote time, energy, and money to: (1) closely monitor their medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

86. Once PII and PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct. Further, the value of Plaintiff and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

87. As a result of Defendant's failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PII and PHI.

88. From a study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[33]

89. With respect to healthcare breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity

---

[33] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KnowBe4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited Oct. 20, 2023).

theft."[34]

90. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[35]

91. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[36]

92. Health information in particular is likely to be used in detrimental ways—by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[37]

93. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[38]

94. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and

---

[34] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HealthITSecurity, https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud (last visited Oct. 20, 2023).
[35] *Id.*
[36] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HealthTech (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.
[37] *Id.*
[38] *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, Experian, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited Oct. 20, 2023).

appropriate security and training measures to protect the PII and PHI of its Customer-Healthcare Providers' patients.

95. Furthermore, Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to unauthorized third parties.

H. Other Impacts of the Data Breach on Plaintiff.

96. Plaintiff Allan Bishop was a patient who receives healthcare services through UF Health Flagler Hospital in St. Augustine, Florida. Plaintiff received a Notice of Data Breach dated December 22, 2023 via U.S. Mail on January 2, 2024 from HEC on behalf of MD Valuecare, LLC. His Notice of Data Breach notes that his data was involved in the breach due to HEC's relationship with MD Valuecare, LLC..

97. Plaintiff was incredibly surprised that the Notice stated that HEC's systems were breached as early as July 2023, given that he did not receive notification until early January 2024.

98. Upon receipt of the Notice, Plaintiff Bishop researched the companies listed in the Notice, conducted a self-investigation and reached out to counsel. Plaintiff set up fraud alerts and confirmed his pre-existing credit monitoring with TransUnion, Equifax and Experian were still active. Plaintiff also changed passwords on his computer and contacted United Healthcare, who offered additional protection through Allstate Identity Protection for a monthly fee.

99. Plaintiff further signed up for additional free credit monitoring through his wife's retirement plan given his concerns regarding his PHI's availability in the public domain.

100. To date, Plaintiff has spent significant time researching the Data Breach and mitigating the impact of the breach on his life, including mitigating his potential economic

damages and other harm resulting from the Data Breach.

101. Despite these efforts, Plaintiff has already seen an increase in spam email and text messages he receives. Plaintiff noticed that this was a considerable increase from the amount of spam emails and text messages that he received prior to the Data Breach.

102. Due to the sensitivity of the PHI compromised in the Data Breach, Plaintiff is and will continue to be at an imminent and certainly impending risk for fraud and identity theft, and their attendant damages for years to come.

CLASS ALLEGATIONS

103. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following class:

> All individuals in the United States whose PII and/or PHI was compromised in the HEC Data Breach announced on or about December 22, 2023 (the "Class").

104. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

105. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when he moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

106. **Numerosity:** Plaintiff is informed and believes, and thereon alleges, that there are at minimum, hundreds of thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through HEC's records,

including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes approximately 6.9 million individuals.

107. **Commonality:** This action involves questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether HEC had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether HEC was negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached its duties thereby;

c. Whether Plaintiff and Class Members are entitled to damages as a result of HEC's wrongful conduct; and

d. Whether Plaintiff and Class Members are entitled to restitution as a result of HEC's wrongful conduct.

108. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. HEC was the custodian of Plaintiff's and Class Members' PII and PHI, when their PII and PHI was obtained by an unauthorized third party.

109. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

110. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of

single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

111. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, HEC's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

112. **Injunctive Relief:** HEC has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23(b)(2).

113. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through HEC's books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

114. Plaintiff restates and realleges the allegations above as if fully set forth herein.

115. HEC owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

116. Defendant's duty to use reasonable care arose from several sources, including but

not limited to those described below.

117. HEC had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By receiving, maintaining, and handling PII and PHI that is routinely targeted by criminals for unauthorized access, HEC was obligated to act with reasonable care to protect against these foreseeable threats. Furthermore, HEC knew or should have known that, if hackers accessed the sensitive data contained in its data systems, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen. Therefore, the Data Breach, and the harm it caused Plaintiff and the Class, was the foreseeable consequence of Defendant's unsecured, unreasonable data security measures.

118. HEC's duty also arose from its position as a business associate. HEC holds itself out as a trusted healthcare business associate, thereby assuming a duty to reasonably protect the information it obtains from its Customer-Healthcare Providers. Indeed, HEC, which receives, maintains, and handles PII and PHI from its Customer-Healthcare providers, was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

119. Additionally, Section 5 of the FTC Act required Defendant to take reasonable measures to protect Plaintiff's and the Class's sensitive data and is a further source of Defendant's duty to Plaintiff and the Class. Section 5 of the FTC Act prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendant of failing to use reasonable measures to protect highly sensitive data. Therefore, Defendant was required and obligated to take reasonable measures to protect data it

possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Defendant's duties to adequately protect sensitive information. By failing to implement reasonable data security measures, Defendant acted in violation of Section 5 of the FTC Act.

120. Similarly, HIPAA is a further source of Defendant's duty to Plaintiff and the Class, as HIPAA required HEC to take reasonable measures to protect Plaintiff's and the Class's sensitive data. Indeed, HIPAA required HEC to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102, *et seq*. By failing to implement reasonable data security measures, Defendant acted in violation of HIPAA.

121. HEC breached the duties owed to Plaintiff and Class Members and thus was negligent. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiff at this time, on information and belief, HEC breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing

to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its clients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

122. But for HEC's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised.

123. As a direct and proximate result of HEC's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to HEC with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as HEC fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

124. As a direct and proximate result of HEC's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

125. Plaintiff restates and realleges the allegations above as if fully set forth herein.

126. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities, such as HEC, for failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendant's duty.

127. HEC violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored and the foreseeable consequences of a data breach involving member PII and PHI obtained from its healthcare provider partners.

128. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

129. The harm that has occurred as a result of HEC's conduct is the type of harm that the FTC Act was intended to guard against.

130. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se.*

131. HEC is an entity covered under the HIPAA, which sets minimum federal standards

for privacy and security of PHI.

132. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et seq.*, and its implementing regulations, HEC had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiff's and the Class members' electronic PHI.

133. Specifically, HIPAA required HEC to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102, *et. seq*.

134. HIPAA also requires HEC to provide Plaintiff and the Class Members with notice of any breach of their individually identifiable PHI "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach." 45 C.F.R. §§ 164.400-414.

135. HEC violated HIPAA by actively disclosing Plaintiff's and the Class Members' electronic PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI; and by failing to provide Plaintiff and Class members with notification of the Data Breach within 60 days after its discovery.

136. Plaintiff and the Class Members are patients within the class of persons HIPAA was intended to protect, as they are members of Defendant's Customer-Healthcare Providers.

137. The harm that has occurred as a result of HEC's conduct is the type of harm that HIPAA was intended to guard against.

138. HEC's violation of HIPAA constitutes negligence *per se*.

139. As a direct and proximate result of HEC's negligence, Plaintiff and Class Members

have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to HEC with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as HEC fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

140. As a direct and proximate result of HEC's negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

141. Plaintiff restates and realleges the allegations above as if fully set forth herein.

142. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statute and state common law as described in this Complaint.

143. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether HEC is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff and the Class continue to suffer injury as a result of the compromise of their PII and PHI and remain at imminent risk that further compromises of their PII and/or PHI will occur in the future.

144. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. HEC owes a legal duty to secure patient PII and PHI obtained from its Customer-Healthcare Providers and to timely notify such patients of a data breach under the common law, Section 5 of the FTC Act, and HIPAA;

b. HEC breached and continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI; and

c. HEC's breach of its legal duty continues to cause harm to Plaintiff and the Class.

145. This Court also should issue corresponding prospective injunctive relief requiring HEC to employ adequate security protocols consistent with law and industry standards to protect patients' (*i.e.*, Plaintiff's and the Class's) PII and PHI.

146. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable

injury, and lack an adequate legal remedy, in the event of another data breach at HEC. If another breach of Defendant's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

147. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to HEC if an injunction is issued. Plaintiff and the Class will likely be subjected to substantial identity theft and other damages. On the other hand, the cost to HEC of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

148. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at HEC, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, prays for relief as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

B. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

C. For damages in an amount to be determined by the trier of fact;

D. For an order of restitution and all other forms of equitable monetary relief;

E. Declaratory and injunctive relief as described herein;

F. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

G. Awarding pre- and post-judgment interest on any amounts awarded; and

H. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: January 9, 2024

Respectfully submitted,

/s/ James E. Cecchi

James E. Cecchi
CARELLA BYRNE CECCHI BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
jcecchi@carellabyrne.com

Gary F. Lynch*
Nicholas A. Colella*
Patrick D. Donathen*
Connor P. Hayes*
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
gary@lcllp.com
nickc@lcllp.com
patrick@lcllp.com
connorh@lcllp.com

Jennifer S. Czeisler*
Edward Ciolko*
STERLINGTON PLLC
One World Trade Center, 85th Floor
New York, NY 10007
Telephone: (212) 433-2993
Jen.czeisler@sterlingtonlaw.com
Edward.ciolko@sterlingtonlaw.com

James M. Evangelista, Esq.*
EVANGELISTA WORLEY LLC
10 Glenlake Parkway, Suite 130
Atlanta, GA 30328
(404)205-8400 office
(404)205-8395 fax
jim@ewlawllc.com

Attorneys for Plaintiff and the Class
**pro hac vice forthcoming*